**DEPARTMENT OF THE ARMY**
UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
UNIT 29351
APO AE 09014-9351

AEAIM-A-P 26 February 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Network Remote-Access Policy

This memorandum expires in 1 year.

1. References:

a. DOD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003 (available at *http://www.dtic.mil/whs/directives/corres/html/85002.htm*).

b. Chairman of the Joint Chiefs of Staff Manual 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), 25 March 2003 (available at *https://ca.dtic.mil/cjcs_directives/cdata/limited/m651001.pdf*).

c. AR 25-1, 31 May 2002, and AE Supplement 1, 29 January 2003, Army Information Management (available at *http://www.apd.army.mil/pdffiles/r25_1.pdf*).

d. AR 25-2, Information Assurance, 14 November 2003 (available at *http://www.apd.army.mil/pdffiles/r25_2.pdf*).

2. The references (para 1) require that Army computers and networks be configured to provide the best security and protection possible. This policy will ensure all personnel in the European theater support the DOD and DA intent to standardize remote-access options and to use better-protected and more cost-efficient access methods.

3. A "remote user" is a person who enters the Army in Europe (AE) NIPRNET from outside the physical or logical boundary of the internal local area network. The remote-access system creates a protected extension of the AE NIPRNET for authorized remote users. The AE NIPRNET remote-access system has the following components:

a. Access to the network. Users will connect through either the Terminal Server Access Control System (TSACS) or a commercial Internet service provider (ISP) that provides dial-up, broadband, wireless, or leased-line services. TSACS and these other network connections provide unencrypted connections to the network.

b. A Virtual Private Network (VPN). The primary function of VPN is to encrypt the path from the user to the network. VPN will allow remote users to—

(1) Protect Army information that is sent and received during remote communications with other users and servers on the AE NIPRNET.

(2) Use the applications available to them in their normal office environment.

4. Remote access to the AE NIPRNET will be used only for unclassified official business. Remote access will never be used to process classified data. Remote users will be subject to monitoring; their connection will be terminated if it causes damage to any part of the network or if their computer is not configured correctly. Personnel who abuse or misuse remote-access capabilities may be disciplined in accordance with the Uniform Code of Military Justice (UCMJ) or Office of Personnel Management (OPM) directives and may have their remote-access account terminated.

5. The 5th Signal Command will—

a. Manage all remote-access points. Before 31 July 2004, personnel currently operating remote-access equipment must pass operational control to 5th Signal Command or terminate operation of the equipment. The 5th Signal Command and each unit passing operational control will negotiate a service level agreement (SLA) as part of the transition plan and implementation. The SLA will establish minimum services that must be provided and unit-unique mission requirements that must be met.

b. Configure all remote-access equipment to require authentication and encryption. The VPN component of the remote-access system provided by 5th Signal Command became fully operational on 1 January 2004. By 31 July 2004, VPN functionality on remote-access equipment will be required. This gives users from now until the end of July to become familiar with VPN's configuration and operating capabilities.

6. Only commanders who are captains and above or supervisors in the grade of GS-13 and above may approve requests for remote access. These approval authorities will also be responsible for—

a. Pre-approving reimbursement for temporary duty (TDY) or remote-access connection charges at the user's home station.

b. Setting specific limits when pre-approving reimbursement for connection charges (a above). Generally, home-station remote-access users should not be reimbursed because they normally can return to their office.

c. Paying approved reimbursements for remote-access charges with internal operations and maintenance (O&M) funds.

7. Information management officers (IMOs) will—

a. Revalidate all current TSACS users for the new remote-access system before 1 August 2004.

b. Use the appropriate AE Remote-Access Request Form (AE Form 25-1H or AE Form 25-1K) to request approval for remote access (AE Suppl 1 to AR 25-1) for current and new users.

c. Keep the completed forms (b above) in unit records and coordinate new and deleted accounts with the supporting network service center (NSC).

8. Employee-owned information systems (EOIS) are prohibited from connecting to the Army network for any purpose. If the approving authority determines that a person has a need for remote-access, then that authority must provide a Government-owned information system (GOIS). Information management officers and remote-access users will complete AE Form 25-1K (AE Remote-Access Computer-Security Compliance Inspection) to ensure the GOIS to be used for remote access is correctly configured.

9. The USAREUR G6 will issue an operation order through the USAREUR G3 to provide detailed implementation instructions on network remote access.

10. POCs:

a. For implementation: Mr. Lewis, DSN 380-4451 or e-mail: lewisb@hq.5sigcmd.army.mil.

b. For policy: Mr. LaChance, DSN 370-7395 or email: daniel.lachance@us.army.mil.

FOR THE COMMANDER:

WILLIAM E. WARD
Lieutenant General, USA
Deputy Commanding General/
Chief of Staff

DISTRIBUTION:
C (AEPUBS)